The Information Society Alliance
EURIM

Summary Report of the Directors' Round Table on Information Governance, 1600-1800, 24th November 2008, The Boothroyd Room, Portcullis House, Westminster

Chair: Stephen Darvill (Logica)
Raporteur: Edward Phelps (EURIM)

SUMMARY OF ROUND TABLE STATEMENTS AND DISCUSSION

1. Statement 1

1.1 A report published by HM Treasury developed the idea that it is critical to put the consumer first, second and third. This was different to the thinking of the political parties, and to the actions of consumers who tend to divulge their personal data on- and off-line, and offer frequent opportunities to compromise their identity.

1.2 Companies have seen that the management of personal data is something which will ideally make them more effective, give them more data about consumers' behaviour and sell more products. Consumers need identity assurance – to be able to assure their identity with ease and confidence. This need will increase over time.

1.3 Organisations can achieve so much in identity management systems without being good at governance. But good governance must be part of any system which delivers what consumers need, which is identity assurance. If you roll forward 20 years, societies that are brilliant at identity assurance will see not just a consumer led advantage, but an economic one. There should be total clarity about what data should be used for, and this should be based on genuinely informed consent, not just some tick box in the small print.

1.4 When we hold personal data in systems, that data should be minimised. We should zealously guard the identity of the persons whose data we have and we do that best by minimising data. Swift accurate means of reporting compromises are critical. Governance of these systems should inspire trust in the security of the data. No-one should consider that they are exempt from the need to inspire trust in this way. Consumers' interests are best served by the adaptation of information standards to large scale systems.

1.5 There is a need for a core alliance between the public sector and organisations that are currently dependent on operating the most effective large scale identity management and assurance systems – most particularly the banks. It's not in consumers' interests for organisations to operate independently and separately.

2. Statement 2

2.1 The potential loss of confidence in the public and private sector's ability to look after large aggregations of data is very worrying and very damaging. Governance is much more about people and processes than technology.

2.2 Good systems architecture and fit-for-purpose encryption are very important and necessary but not sufficient. Winning hearts and minds is more critical that the technology. Good practice has to come from the top of the organisations. Education and training is best achieved by embedding it in "board dilemma" courses, where people look at problems like IT-enabled business change.

2.3 In 2004, 64% of IT directors named their top worry as IT security. In 2007, that went up to 78%. More effort is needed from all three parties in communicating where information sharing would be beneficial.

3. Statement 3

3.1 Information governance relies on several things. Clear responsibility, accountability and authority for information management; training for all staff; clear understanding and management of the processes associated with the introduction of databases. Appropriate security systems for their protection. Simple clear documentation on the organisation's use and dependence on information, that is followed through the organisation.

3.2 A significant problem with ever-larger databases is associated with the stewardship of the data held. Problems multiply where data integrity is poor and you try and share it and match it.

3.3 A data holding organisation also has to ensure that data is the minimum needed for its purposes. It must have accuracy, retention time and the relevant expiry date. The integrity of the data, particularly personal data, must be maintained throughout the life cycle. That is not easy. The collecting organisation must have consent, and consent to share it with third parties. It has got to pass on obligations associated with the data to everyone it shares it with. This is no easy task.

3.4 We must be very careful about personal data that is no longer required to support a business purpose. It is incredibly difficult to safely dispose of data – an issue that is commonly neglected.

4. Statement 4

4.1 If Facebook was a country, it would equal the size of Russia, and it is doubling every 16 months. Is the ability of senior executives accelerating at the same rate as technical innovations? Our level of understanding in terms of technology is in fact deviating from our ability to keep track of what that technology is doing. The rate of change of the issues is accelerating with the technology, and the rate of growth is not going to decelerate.

4.2 The issue of personal data protection will be with us forever. More than 65% is outsourced from the design, building and running of the main core systems, and the private and public sectors will share equally in success - or failure.

4.3 Information assurance is another issue. Nobody wants a big device to carry around for identity or authentication purposes, but it's not about technology, it's about people who do not track their data enough. They need to execute known procedures and policies. Generally we all know the rules, but for whatever reason, we choose not to execute them. We are not short of policy – but we choose not to follow it, and frequently fail to execute good practice. We can encrypt to our heart's content, but at some point somebody needs to un-encrypt the data to do something with it. However, we have been removing opaqueness and fixing some of the issues around information governance. We are making sure chief executives fully understand that they are accountable for information loss, and that the information risk owners attend board meetings. 500,000 civil servants are currently being trained how to manage data.

4.4 The moment we run off in different directions we lose as a team. If we get to the situation where citizens lose faith in terms of what organisations do with their data, it impacts on the prosperity of the UK.

5. Statement 5

5.1 If we do not solve the problem at a fundamental level, throwing money at it will not solve it. Having accountability: individuals may fear running into the CEO because some day they may be asked about the state of security and protection, when they don't have a clue about how to respond or measure it.

5.2 We need a standard that allows us to do this. We need a consistent method for measuring the state of security, presenting empirical data, and communicating it. We are taking the first steps that are needed from the vendor community to build the products that become solutions. It has to give a fundamental way to change the industry, and the way to force that hand is to create security at the very beginning. CIO's should use their buying power to change the way vendors operate.

6. Discussion

6.1 It is questionable whether as a nation we have the culture of responsibility which should underpin information management. There is a level of personal as well as public responsibility. The most important thing is that individuals want confidence in the way that their data is going to be managed and shared. Maybe we need something that allows people to think a little bit more about the importance of the data and the damage that failure to apply the appropriate standards can do, where that can lead us, and what the consequences might be.

We need to develop a culture of putting the consumer first, and ensuring secure and safe practices around the quality and handling of data.

6.2 We have not been open enough in asking what public attitudes are towards the sharing of data. What is really important for the next six months to a year is trying to understand what the public wants.

6.3 We have heard a lot about culture and people. The outcome depends on where you are starting from. If you are dealing with excluded people, their confidence in public authority is low to start with. In terms of technical and cultural change there are unlikely to be too many answers. We should be looking towards establishing some principles rather than solutions.

6.4 On economic advantage: we have looked at 1,000 organisations around the world and tried to benchmark around the use of information. We looked at people, process, technology and culture. The private sector is generally further ahead in the people, process and culture categories, and in the technology category the government is, so it is not a technology issue. It is very much around treating data as a strategic asset.

6.5 We should distinguish between the public and the private sector: if the private sector makes mistakes it risks losing trust. In the case of Enron, the business had gone by the time the court case had arrived. The penalty that the market place can execute in a competitive environment far exceeds any regulation.

6.6 We are always encouraging companies to manage risk. There is a real incentive in the private sector to manage this much more carefully. But in the public sector there is probably more value in sharing more information. The issue is how not to have something that is the same for both sectors, but how you can differentiate, how you incentivise the public sector to share better. This means penalties.

6.7 Sharing is less beneficial in the private sector than it is in the public sector. It is virtually impossible in this country to purchase something without ticking the box.

6.8 Controls should not apply to the private sector because the market mechanisms will provide these. There is very rarely a commercial interest in telling your customers that you have been sloppy with their data. We need something that requires that to happen to signal to the market, so it will discriminate in such a way to ensure that people will behave appropriately.

6.9 The market will respond once people know that a particular company is repeatedly having to send out alerts. While there are large areas of industry that behave extremely responsibly, where you can rely on the best possible standards being achieved, there has to be some failsafe for those who are less responsible.

6.10 In the voluntary sector people act as a bridge between those who are prepared to engage with the public sector and those who are not. It is a social cohesion issue.

6.11 A partnership between the public and the private sector needs to look at ways of giving consumers a consistent way of verifying themselves.

6.12 Do Boards really understand the value of what they have? If data is to be treated as a strategic asset, we have to look at it in a different way. But if data is not shared because of fear, there is potential for a ‘data crunch’. We must treat data as an asset, and make sure it can be exploited and shared effectively: this will be fundamental to how society will operate successfully in the future.

6.13 The idea that we own our personal data is now central, but is this true? If you go back 100 years, the BACS records belonged to the banks. This use of language – our personal data as property, has altered the debate.

We should question if we are making the right assumption. When we look at information as an asset that needs to be controlled, we ignore the benefits of sharing. Huge value may ensue from sharing information.

6.14 The data *is our* data. Solutions to encryption should be based on that understanding, in particular where government is using data about individuals. If it is not our data, whose is it? For example, if we were to argue that data belongs to the NHS not the individual, this would represent a significant shift in the relationship between the government and the governed.

6.15 It is interesting that the data protection directive is all about procedure and culture, and remarkably little about the data subject. Current legislation starts from the wrong end. You can hold data as much as you like but if the citizen is damaged as part of your actions, you are subject to civil and criminal legislation.

6.16 Given that the government has a very ambitious programme for cross departmental and cross agency sharing, the onus is on government to establish that the necessary security is available. In the past, the government has moved ahead with data sharing before being confident that it is secure. People like the information commissioner are catching up with what the government is doing: moving ahead without being confident.

6.17 One question we should address is whether technology is overtaking us and our capacity to manage risk? One common sense recommendation is no more reviews. We need to ask is this a solvable problem?

Technical capability will continue to grow exponentially. It is important to grow a culture with an expectation of behaviours which provide guidance whatever the technology does.

6.18 Reviews are very important. Unlike the private sector, government is dealing with every citizen: this means over one hundred different languages, and with that comes different cultural norms. It is not true to say we are running ahead without noticing what is going on.

6.19 The Police National Computer is 33 years old on April 1 next year. That does a great deal of necessary sharing. The government has always been ahead. But there is an issue in terms of ability to re-equip ourselves for the consequences of what we are inventing.

6.20 There has to be a level of education that is compulsory. Are individuals fully aware of where their actions will lead? Technology will always run away from us, but hopefully there will always be people to catch up with it.

6.21 We need to be focussed on the outcomes that we want to see, and this may best be achieved using incentives. Remote places in the UK and overseas are now delivering private and public sector services. We need to translate things into parameters, and we need to be able to measure outcomes, although there is some way to go.

6.22 We are not short of guidance and standards and it can be difficult to keep pace with what already exists. There is a balance to be struck because not sharing data also causes damage. There is a connection between good use of data and organisational performance. We should not forget that.

6.23 The pace at which fraudulent transactions can be made makes us increasingly conscious of what is happening to our data. The consumer should provide consent for how his personal data is used. But who should designate when consent should be released?

6.24 Data has to have more context in the future than it has today. That has to be associated around a particular purpose. We must be able to ensure it does not get misused in the wrong context.

6.25 There are some simple, practical things we can do to make sure citizens know what they are getting into. The cost of a mandatory data breach notification requirement the exposure involved seems to be a major incentive to improve internal processes.

6.26 Social networking sites should only release personal data, where permissions exist. This is a complex issue that is going to get more important as we move towards internal advertising, because the bulk of services are free.

Social networking is on the whole consensual, but government data sharing is not necessarily consensual. Of course people cannot ask to be taken off the criminal records database, but there are many things the government thinks it wants to do for us. We ought to be able not to be involved. The governance of the public sector does have some very important differences from database governance in other places.

6.27 We have a collective responsibility about cooperation and engagement with the public. How does the consumer consent to something that is as fast moving as the internet? If we are not careful we end up with more regulation and more legislation. The tendency is to combat the causes of the last disaster but the whole process takes so long that the technology has moved on several years by the time this is finished.

6.28 There is a worrying track emerging, where the rules and regulations that people are driving forward disenfranchise the voluntary sector.

6.29 Every time there is a data loss, people lose trust in the government, while at other times there is a demand to share everything. Such large and potentially dangerous fluctuations in the public view make it difficult to get the issue right.

6.30 There should be more anonymisation of data that needs to be traded but does not need to be linked to an identity. We should take information management out of data sharing wherever possible to make it less worrying. It is crucial to establish that there will be clear guidelines for the sharing of information. Individuals should be in control wherever possible.

6.31 The Chair concluded by suggesting that EURIM would be working to produce a forward programme based on the ideas raised at the meeting and that we would welcome the involvement of all present.